AMENDMENTS TO THE CLAIMS

1. (Previously presented) A secure data authentication apparatus to authenticate a software file, the software file having a first signature appended to the software file, for use on a computer system, wherein said computer system is assigned an owner key that is unique to said computer system, said first signature comprising a source hash value that is computed by processing at least some of said software file using a selected hash function, which source hash value is encrypted using said owner key to produce said first signature, the apparatus comprising:

a secure processing device within the computer system to receive the software file and hash the software file using said selected hash function to produce a first hash value; and

a first key located within the secure processing device, which first key comprises said owner key wherein the secure processing device encrypts the first hash value with the first key to generate a second signature and compares the first signature with the second signature, and if the first signature matches the second signature, the computer system accepts the software file as being authenticated.

2. (Previously presented) The secure data authentication apparatus of claim 1 wherein the software file further comprises a first source signature appended to the software file, the apparatus further comprising:

a source key located within the secure processing device, wherein the secure processing device encrypts the first hash value with the source key to generate a second source signature and compares the first source signature with the second source signature, and if the first source signature matches the second source signature, the computer system accepts the software file as being authenticated from the source represented by the first source signature.

3. (Previously presented) The secure data authentication apparatus of claim 1 wherein the software file further comprises a first owner signature appended to the software file, the apparatus further comprising:

an owner key located within the secure processing device, wherein the secure processing device encrypts the first hash value with the owner key to generate a second owner signature and compares the first owner signature with the second owner signature, and if the first owner signature matches the second owner signature, the computer system accepts the software file as being authenticated.

4. (Previously presented) The secure data authentication apparatus of claim 1, further comprising:

a key exchange request having a first key exchange signature appended thereto, the key exchange request sent from the computer system to the secure processing device, wherein the secure processing device hashes the key exchange request to generate a second hash value;

a first key exchange key located within the secure processing device, wherein the secure processing device encrypts the second hash value with the first key exchange key to generate a second key exchange signature and compares the first key exchange signature with the second key exchange signature, and if the first key exchange signature matches the second key exchange signature, the secure processing device erases the first owner key; and

a second owner key within the key exchange request, wherein the secure processing device saves the second owner key.

5. (Previously presented) The secure data authentication apparatus of claim 4 wherein the computer system further comprises a first feature file and the computer system performs in accordance with the first feature file, the apparatus further comprising:

a second feature file having a third owner signature appended thereto, wherein the secure processing device hashes the second feature file to generate a third hash value which is encrypted with the second owner key to generate a fourth owner signature and compares the third owner signature with the fourth owner signature, and if the third owner signature matches the fourth owner signature, the computer system replaces the first feature file with the second feature file.

6. (Previously presented) The secure data authentication apparatus of claim 1 wherein the program comprises a feature file having a plurality of features wherein a subset of the plurality of features are activated and the computer system operates in accordance with the subset of the plurality of features.

7. (Previously presented) A secure data authentication apparatus to authenticate an owner of a software file and of a telephony switching system on which the software file is stored, the apparatus comprising:

a first feature file and a software file, the first feature file having a plurality of features and a first owner signature appended thereto, wherein said telephony switching system is assigned a first owner key that is unique to said telephony switching system, said first owner signature comprising a source hash value that is computed by processing at least some of said software file using a selected hash function, which source hash value is encrypted using said first owner key to produce said first owner signature, wherein a first subset of the plurality of features is activated;

a secure microprocessor within the telephony switching system, the secure microprocessor having an encryption algorithm, wherein the secure microprocessor hashes the first feature file using said selected hash function to generate a first hash value; and

a first owner key within the secure microprocessor, wherein the secure microprocessor encrypts the first hash value with the first owner key to generate a second owner signature and the secure microprocessor compares the first owner signature with the second owner signature, and if the first owner signature matches the second owner signature, the telephony switching system operates in accordance with the first subset of the plurality of features of the first feature file.

8. (Previously presented) The secure data authentication apparatus of claim 7, the apparatus further authenticating a source of the software file, the apparatus further comprising:

a first source signature appended to the first feature file; and

a source key located within the secure microprocessor, wherein the secure microprocessor encrypts the first hash value with the source key to generate a second source signature and the secure microprocessor compares the first source signature with the second source signature, and if the first source signature matches the second source signature, the telephony switching system operates in accordance with the first subset of the plurality of features of the first feature file.

9. (Previously presented) The secure data authentication apparatus of claim 7, further comprising:

a second feature file having a second subset of the plurality of features activated, the second feature file having a third owner signature appended thereto; wherein the secure microprocessor receives the second feature file and hashes the second feature file to generate a second hash value and encrypts the second hash value with the first owner key to generate a fourth owner signature, and the secure microprocessor compares the third owner signature with the fourth

owner signature, and if the third owner signature matches the fourth owner signature, the second feature file is written over the first feature file.

10. (Previously presented) A method for authenticating an owner of a software file that has a first identification code comprising a source hash value that is computed by processing at least some of said software file using a selected hash function, which source hash value is encrypted using an owner key to produce said first signature, attached thereto for use on a computer system, wherein said computer system is assigned said owner key that is unique to said computer system, the computer system comprising a secure processor having an encryption algorithm and an owner key, the method comprising:

initiating the computer system;

hashing the software file using said selected hash function within the secure processor to generate a first hash value;

encrypting the first hash value with the owner key to generate a second identification code; and

comparing the first identification code with the second identification code, and if the first identification code matches the second identification code, the computer system accepts the software file as being authenticated for the owner's use.

11. (Previously presented) A method for authenticating an owner of a software file that has a first owner signature comprising a source hash value that is computed by processing at least some of said software file using a selected hash function, which source hash value is encrypted using an owner key to produce said first signature, appended to the software file, for use on a computer system, wherein said computer system is assigned said owner key that is unique to said computer system, having a secure processing device to generate an authorization signal, the secure processing device comprising a security routine, an encryption algorithm and a first owner key, the process comprising:

receiving the software file by the computer system and sending the software file to the secure processing device;

hashing the software file using said selected hash function to generate a first hash value;

encrypting the first hash value within the secure processing device with the first owner key to generate a second owner signature; and

comparing the first owner signature to the second owner signature, wherein if the first owner signature and the second owner signature match, the secure processing device generates the authorization signal.

12. (Previously presented) The method for authenticating an owner of the software file of claim 11 wherein the software file further comprises a first source signature appended thereto and the secure processing device further comprising a source key; the method further authenticating a source of the software file, the method comprising:

encrypting the first hash value within the secure processing device with the source key to generate a second source signature; and

comparing the first source signature to the second source signature, wherein if the first source signature and the second source signature match, the secure processing device generates the authorization signal.

13. (Previously presented) The method for authenticating an owner of the software file of claim 11 wherein the secure processing device further comprises a first key exchange key, the method further comprising:

receiving a key exchange request by the secure processing device, the key exchange request including an encrypted second owner key and having a first key exchange signature appended thereto;

hashing the key exchange request to generate a second hash value;

encrypting the second hash value with the first key exchange key to generate a second key exchange signature; and

comparing the first key exchange signature with the second key exchange signature, wherein if the first key exchange signature and the second key exchange signature match, the secure processing device decrypts the second owner key and replaces the first owner key with the decrypted second owner key.

14. (Previously presented) The method for authenticating an owner of a software file of claim 13 wherein the key exchange request further comprises an encrypted second key exchange key, the authenticating method further comprising:

decrypting the encrypted second key exchange key with the first key exchange key; and

replacing the first key exchange key located within the secure processing device with the decrypted second key exchange key.

15. (Previously presented) The method for authenticating a source and an owner of a software file of claim 13 wherein the computer system further comprises a first feature file having a first plurality of features, wherein a first subset of the first plurality of features is activated and the computer system performs in accordance with the first subset of the first plurality of features, the method further comprising:

receiving a second feature file having a third owner signature appended thereto, the second feature file comprising a second plurality of features wherein a second subset of the second plurality of features is activated;

hashing the second feature file within the secure processing device to generate a third hash value;

encrypting the third hashed file with the second decrypted owner key within the secure processing device to generate a fourth owner signature; and

comparing the third owner signature with the fourth owner signature, wherein if the third owner signature matches the fourth owner signature, the computer system overwrites the first feature file with the second feature file, and the computer system performs in accordance with the second subset of the second plurality of features.

Claims 16 and 17 (Canceled)

18. (Previously presented) A method for authenticating a software file from a PBX manufacturer, the software file comprising a feature file having a plurality of features wherein a subset of the plurality of features are activated, the software file operating on a PBX, the PBX comprising a secure microprocessor having an encryption algorithm and a first key that is unique to said PBX, the method comprising:

hashing the feature file using a selected hash function at the PBX manufacturer to generate a first hash value;

encrypting the first hash value with said first key to generate a first signature;

appending the first signature to the feature file;

receiving the feature file and appended first signature by the secure microprocessor;

hashing the received feature file using said selected hash function within the secure microprocessor to generate a second hash value;

encrypting the second hash value with the first key to generate a second signature; and

comparing the first signature with the second signature, and if the first signature matches the second signature, the PBX accepts the software file as being authenticated.